RESTECH SOLUTIONS

CYBER RESILIENCE WITH DATA BACKUPS

When it comes to working with supply chain or third-party vendors, complete data security is never a guarantee. That's why you need to have a comprehensive data protection and backup plan that includes both disaster recovery and business continuity measures.

To ensure your data is protected from cyber risks emanating internally or from your supply chain, we recommend implementing these backup strategies:

Get to Know Your business

- Infrastructure and IT systems
- Business-critical operations, SaaS applications, data assets
- Main or priority customers
- Essential staff and supply chain vendors

Business Impact Analysis and Risk Assessment

- Security risks and worst-case scenarios
- Likelihood of failures and high-vulnerability points
- Recovery Point & Time Objectives (RPO & RTO)
- Compliance obligations and requirements

RESTECH SOLUTIONS

Define Your Resilience Strategy

- Incident response strategy
- Key personnel and supply chain contacts and responsibilities
- Data and system recovery processes
- Business continuity planning

Establish Your Recovery & Continuity Plan

- Clearly document all steps, contact details and procedures in a comprehensive policy plan
- Distribute and train personnel and vendors thoroughly

Regular Testing & Continuous Monitoring

- Regular testing and 'fire drills' to ensure your resilience plans are effective and optimized for whenever you should need them
- Processes for vetting and monitoring supply chain risk and cybersecurity practices

Strengthen Your Data Security Posture With Data Backups

We specialize in helping protect organizations just like yours from data loss, disasters and disruptive incidents. Save yourself from a world of stress and frustration and ensure your data protection plan is designed for effective cyber resilience.

CONTACT US TODAY

713-936-6855
info@restech.solutions
https://restech.solutions/contact